ALIBABA CLOUD

阿里云

数据库审计
用户指南（C100）

文档版本：20201103

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.常用操作导航

本文介绍了云盾数据库审计系统C100的常用操作，便于您参考。

- 启用数据库审计实例：开通数据库审计后，启用实例。
- 管理数据库审计实例的标签：通过标签实现实例的分类和批量管理。
- 管理数据库审计实例：管理实例，包括设置公网白名单、升级配置、修改存储设置和续费等操作。
- 登录数据库审计系统：登录数据库审计系统。
- 管理数据库：在数据库审计系统中添加、编辑、删除数据库。
- 部署Agent程序：在用户终端或目标数据库服务器上部署Agent程序，使数据库审计服务收集目标数据库的访问流量信息。
- 审计经典网络数据库实例：通过ClassicLink功能，实现审计经典网络中的数据库实例。
- 查询分析：数据库审计系统提供不同类型的日志供您查询。
  - 审计日志：查询所有审计数据。
  - 告警日志：查询数据库的告警信息。
  - 会话日志：查询客户端与服务器端之间建立的会话信息。
- 规则配置：为数据库配置并启用审计规则后，命中规则的审计记录会触发告警；支持配置系统内置审计规则和自定义审计规则。
  - 为数据库配置审计规则
  - 管理用户规则和白名单
- 报表中心：在数据库审计系统中查看、订阅、导出报表，和管理订阅任务。
- 系统管理：管理数据库、管理Agent和重置偏好设置。

2.启用数据库审计实例

购买数据库审计实例后，您需要启用实例，才能登录数据库审计系统并使用审计服务。

操作步骤

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**数据库审计（C100）**。
3. 在**我的审计**页面，定位到需要启用的数据库审计实例，单击其**操作**列下的**启用**。

   > **说明** 只有实例的状态为**未初始化**时，才能在实例的**操作**列下进行启用操作。

   

4. 在**实例启用**对话框中，选择实例的专有网络和虚拟交换机，并单击**确定**。

   > **说明** 专有网络和交换机设置在实例启用后无法修改，请您根据以下情况选择实例的专有网络。
   >
   > - 审计对象为ECS自建数据库时，选择该ECS所在的专有网络。
   > - 审计对象对于RDS实例时，选择与RDS实例连接的应用服务器所在的专有网络。

   

执行结果

成功启用实例后，实例的状态更新为运行中。

3.管理数据库审计实例的标签

数据库审计提供标签管理功能，方便您标记数据库审计实例资源，实现分类批量管理。

背景信息

每个标签都由一对键值对（标签键和标签值）组成，数据库审计实例标签存在以下使用限制：

- 一个实例最多可以绑定20个标签。
- 一个实例的每个标签的标签键必须唯一，相同标签键的标签值会被覆盖。
- 不支持未绑定实例的空标签存在，即标签必须绑定在某个数据库审计实例上。

为实例添加新标签

参考以下操作步骤，为数据库审计实例添加标签：

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**数据库审计（C100）**。
3. 在**我的审计**页面，定位到需要添加标签的数据库审计实例。
4. 鼠标移动到实例的**标签**栏图标上，单击**编辑**标签。

5. 在**标签管理**对话框中，单击**新增标签**。
6. 输入**标签键**和**标签值**，单击**确定**。

> **说明** 您可以在编辑标签对话框中为目标添加多个标签。

7. 单击**确定**，完成添加标签的操作。

为实例选择已有的标签

参考以下操作步骤，为数据库审计实例选择已有的标签：

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**数据库审计（C100）**。
3. 在**我的审计**页面，定位到需要添加标签的数据库审计实例。
4. 鼠标移动到实例的**标签**栏图标上，单击**编辑**标签。

5. 在**标签管理**对话框中，单击**选择已有标签**。
6. 选择标签键和标签值。

7. 单击**确定**，完成选择已有标签的操作。

通过标签搜索实例

参考以下操作步骤，搜索拥有指定标签的数据库审计实例：

1. 登录云盾数据库审计控制台。

2. 在左侧导航栏中，选择**数据库审计（C100）**。
3. 在**我的审计**页面，从标签下拉栏中选择标签键和标签值。

4. 在实例列表中，查看符合该标签的所有实例。

删除实例的标签

参考以下操作步骤，删除指定数据库审计实例的标签：

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**数据库审计（C100）**。
3. 鼠标移动到实例的**标签**栏图标上，单击**编辑**标签。

4. 在标签设置对话框中，单击要移除的标签的删除图标。

5. 单击**确定**，完成删除标签操作。

> **说明** 数据库审计不支持批量删除多个实例的标签，您只能单独删除某一个实例的标签。

4.管理数据库审计实例

购买数据库审计实例后，您可以在云盾数据库审计管理控制台管理您的数据库审计实例。

操作步骤

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**数据库审计（C100）**。
3. 在**我的审计**页面，查看已开通的数据库审计实例的地域、状态、网络、**版本**、**到期时间**等信息。

4. 管理数据库审计实例。
   - 配置网络白名单

     单击**配置白名单**，您可以配置公网访问白名单。

     

   - 规格升级购买

     在**版本**区域，单击**升配**，并在提示框中单击**确定**，您可以在购买页面升级数据库审计实例的规格和存储的空间。

     

   - 存储管理

     在**存储信息**区域，单击**配置**，可以进行存储空间的清空和存储时长的调整，同时您可以将您的审计记录备份到OSS。

     > **说明** **存储时长**不能小于30天或大于185天。

     

   - 续费

     在**到期时间**区域，单击**续费**，您可以为该数据库审计实例续费，延长该实例的服务时长。

     > **说明** 数据库审计实例到期后将无法续费，请您关注数据库审计实例的到期时间，并在实例到期前根据需要续费。

5.登录数据库审计系统

本文介绍了在启用C100数据库审计实例后，如何登录数据库审计系统的具体操作。

前提条件

已启用C100系列数据库审计实例，具体操作参见启用数据库审计实例。

操作步骤

1. 登录云盾数据库审计控制台。
2. 在顶部区域下拉框中，选择数据库审计实例所在的地域。

3. 在左侧导航栏中，选择**数据库审计（C100）**。
4. 在**我的审计**页面，定位到要登录的实例， 单击其**操作**列下的**管理**。

执行结果

成功登录数据库审计系统，进入数据库审计系统的**总览**页面。

后续步骤

完成配置向导，具体操作请参见C100快速入门。

6.管理数据库

本文介绍了在数据库审计系统中添加、编辑、删除数据库的具体操作。在进行数据库审计前，您必须在数据库审计系统中添加要审计的数据库。已添加的数据库支持编辑和删除操作。

支持的数据库类型

数据库审计系统支持对ECS自建数据库和RDS云数据库进行审计。

- ECS自建数据库

  对于在ECS云服务器上自建的数据库，数据库审计系统支持国内外各类主流数据库，具体支持的数据库版本请参见下表。

数据库	版本
Oracle	8i、9i、10g、11g、12c、18c、19c
MySQL	4.0、4.1、5.0、5.1、5.5、5.6、5.7、8.0
SQL Server	2000、2005、2008、2012、2014、2016、2017
Sybase	11.9、12.5
DB2	V80、V81、V82、V95
Informix	IDS 9
Oscar	5.5、5.7
达梦（DM）	DM7
Cache	所有版本
PostgreSQL	9、10、11
DCOM	所有版本
Teradata	所有版本
人大金仓（Kingbase）	V6
GBase	8.5a、8.8s
MariaDB	5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3
WEB	所有版本
FTP	所有版本
SMTP	所有版本
POP3	所有版本

数据库	版本
Hana	1
MongoDB	2.x、3.x、4.x
HBase (protobuf)	所有版本
HBase (thrift)	thrift1、thrift2
Hive	所有版本
Redis	所有版本
Elasticsearch	所有版本
Cassandra	3.X
HDFS	所有版本
Impala	3.X
GaussDB	100、200、300

- RDS云数据库

  对于RDS云数据库，数据库审计系统支持的版本情况请参见以下表格。

数据库	版本
MySQL	5.5、5.6、5.7、8.0
SQL Server	2008、2012、2016、2017
PostgreSQL	9、10、11
MariaDB	10.3

添加数据库

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**资产 > 资产管理**。
3. 单击左上角的**新增**。

   

   > **说明** 您也可以在**总览 > 仪表盘**页面，单击**资产主要指标**模块的**新增**。

4. 在**新增资产**页面，完成数据库配置，并单击**保存**。
   - 添加RDS实例

     

RDS实例配置

参数	是否属于最简配置模式	说明
类型	是	选择**RDS**，并选择要审计的RDS实例的类型和版本。
实例名	是	选择要审计的RDS实例ID。
资产组	是	选择要审计的RDS归属的资产组，默认为缺省资产组。您可以单击右侧**管理**，进行新增、编辑或删除资产组操作。 **说明** 缺省资产组不支持编辑和删除操作。
名称	是	设置数据库名称。选择RDS实例后，默认取RDS实例名作为名称，支持修改。
IP端口	是	选择RDS实例名后自动填写，且不可修改。 **说明** 成功添加数据库后，您可以通过编辑数据库修改数据库的IP和端口，具体操作请参见编辑数据库。
状态	否	选中**启用**或**禁用**当前数据库审计配置。
编码	否	审计数据的编码类型。支持UTF-8、UTF-16等多种类型。默认为**自动识别**。 **说明** 如果您不清楚数据库的编码，可以先不作修改，保留默认值。当审计的内容不正确或包含乱码时，再使用其它编码类型。
流量方向	否	选中**双向审计**或**单向审计**。 ■ 双向审计的审计内容为：请求+客户端信息+服务端信息+返回信息。 ■ 单向审计的审计内容为：请求+客户端信息+服务端信息。不包括返回信息。
保存行数	否	流量方向为双向审计时，设置要保存的返回信息的行数。取值范围：0~999，0表示不保存返回结果。最多支持存储64 KB。
安全证书	否	配置证书和证书密码。您可以选择导入证书或直接复制证书的内容来配置证书。安全证书和证书密码请联系数据库厂商获取。
证书密码	否	

- ECS自建数据库

ECS自建数据库配置

配置项	是否属于最简配置模式	说明
类型	是	选择**通用数据库**，并选择要审计的通用数据库的类型和版本。 **说明** 通用数据库即为ECS自建数据库。
名称	是	设置数据库名称。
操作系统	是	选择数据库服务器的操作系统类型，具体取值与数据库类型有关。
IP端口	是	填写数据库的IP地址和端口。单击**增加IP与端口**可以增加多条记录。 **说明** 在Oracle RAC或MySQL读写分离等场景中，您可以添加多个IP和端口，实现对整个集群的审计。
状态	否	选中**启用**或**禁用**当前数据库审计配置。
编码	否	审计数据的编码类型。支持UTF-8、UTF-16等多种类型。默认为**自动识别**。 **说明** 如果您不清楚数据库的编码，可以先不作修改，保留默认值。当审计的内容不正确或包含乱码时，再使用其它编码类型。
流量方向	否	选中**双向审计**或**单向审计**。 ■ 双向审计的审计内容为：请求+客户端信息+服务端信息+返回信息。 ■ 单向审计的审计内容为：请求+客户端信息+服务端信息。不包括返回信息。
保存行数	否	流量方向为双向审计时，设置要保存的返回结果的行数。取值范围：0~999，0表示不保存返回结果。最多支持存储64 KB。
安全证书	否	配置证书和证书密码。您可以选择导入证书或直接复制证书的内容来配置证书。安全证书和证书密码请联系数据库厂商获取。
证书密码	否	

> 说明
>
> - 如果需要一次性添加多个数据库，您可以选中**保存后不关闭，继续添加数据库**。这样设置后，在完成数据库配置并单击**保存**后，可以继续添加下一个数据库。
> - 默认启用最简配置模式，最简配置模式下的配置项均为必填项，您可以单击**更多配置**，切换为更多配置模式。如无特殊需求，建议您使用最简配置模式添加数据库。
> - 更多配置模式下，您可以进行全面配置（例如单双向审计配置），单击**最简配置**，可以切换回最简配置模式。
>
>   单双向审计配置：添加数据库后，系统默认采用双向审计，且审计结果不保存；您可以在单双向审计配置中选用单向或双向审计，并设置（双向审计时）审计结果的保存数量。

成功添加数据库。已添加的数据库显示在**资产 > 资产管理**页面。您也可以在**总览**页面的**资产卡片**下看到已添加的数据库。

添加数据库后，您还需要在数据库服务器上部署数据库审计的Agent程序，才能开启采集审计数据。具体操作请参见部署Agent程序。

编辑数据库

已添加到数据库审计系统中数据库配置发生变化时，您需要在数据库审计系统中更新数据库信息。

1. 登录云盾数据库审计系统。 具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，选择**资产 > 资产管理**。
3. 定位到要编辑的数据库，单击操作栏**编辑**。
4. 在**编辑资产**页面，修改数据库配置。数据库的配置详情，请参见添加数据库。

   
5. 单击**保存**。

删除数据库

如果不再需要审计某个数据库，您可以在数据库审计系统中删除数据库。

1. 登录云盾数据库审计系统。 具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，选择**资产 > 资产管理**。
3. 定位到要删除的数据库，单击**删除**。

   

4. 在删除提示页面，单击**确定**，成功删除数据库。

后续步骤

- 添加数据库后，您必须在数据库服务器上部署数据库审计的Agent程序，才能使数据库审计服务收集目标数据库的访问流量信息。具体操作请参见部署Agent程序。
- 添加数据库后，您可以为其配置审计规则，使命中规则的审计记录触发告警。具体操作请参见为数据库配置审计规则。

7.部署Agent程序

数据库审计系统的Agent程序是部署在用户终端或目标数据库服务器上的功能插件，用来转发数据库访问流量到审计系统。您需要根据数据库服务器的操作系统类型，选择部署Linux或者Windows版本的Agent，才能使数据库审计服务收集目标数据库的访问流量信息。

Agent程序的部署位置

根据所添加的数据库类型，您需要将Agent程序部署在以下位置：

- RDS数据库：Agent程序需要部署在与该数据库相连的应用服务器上。

  > **说明** RDS数据库内暂时无法安装配置Agent。

- ECS自建数据库：Agent程序可以部署在数据库所在服务器上，也可以部署在与该数据库相连的Web服务器上。

  > **说明** 如果您的ECS位于经典网络中，请参照审计经典网络数据库实例进行特殊处理。

Linux系统部署Agent

背景信息

云盾数据库审计系统的**系统管理**导航下提供**Agent管理**功能页面，您可以在**Agent管理**页面下载Agent并查看Agent的连接状态。Agent的部署操作在Linux服务器上执行。

针对安装了云助手的Linux系统ECS，您可以通过云助手自动安装Agent，无需登录服务器进行操作。

操作步骤

1. 登录数据库审计系统。具体操作请参见登录数据库审计系统。
2. 前往**系统管理 > Agent管理**页面。
3. 单击**安装Agent**页签，选择通过云助手自动安装Agent或者下载Agent手动安装。

   

   - **通过云助手安装**：针对安装了云助手的Linux系统ECS，推荐您使用该方式。该方式操作简便，Agent安装后自动运行。具体操作如下：
     a. 单击**开始安装**。
     b. 在**通过云助手安装Agent**对话框中，勾选要安装Agent的实例，并单击**安装选中实例**。您也可以单击一个实例操作列下的**安装**，单独为其安装Agent。

        

     c. 等待安装完成。

        成功安装后，目标实例的**Agent状态**更新为**运行中，已连接**。

        

   - **下载Agent手动安装**
     a. 在**下载Agent手动安装**区域，单击**Linux**。
     b. 在**下载**对话框中，等待打包成功，单击**下载**，下载Linux版Agent安装包。

        

c. 登录Linux服务器。

d. 将下载好的Agent安装包上传到Linux服务器的指定目录，用作解压和运行安装脚本。

> 说明
> - 解压目录中不能出现空格。
> - 每次更换运行或解压目录时，需要重新运行安装脚本。

e. 运行以下命令，解压Agent安装包。

```
tar –xf dbagent_V1.0.tar.gz
```

f. 运行以下命令，安装并启用Agent。

```
./install.sh
```

> 说明
> - 禁止直接运行二进制文件。
> - 必须以root账号运行脚本，且指定解释器为bash（或不指定解释器）。

g. Agent安装启用后，回到云盾数据库审计系统，前往**系统管理 > Agent管理**页面，在**查看Agent状态**页签下查看Agent的**连接状态**。

连接状态显示**无异常**，表示成功部署Agent。

更多操作

在Linux环境下，您可以根据需要对已部署的Agent程序执行以下操作：

- 卸载：运行安装目录下的*uninstall.sh*
- 启用：运行安装目录下的*dbagent_start.sh*
- 停用：运行安装目录下的*dbagent_stop.sh*

Windows系统部署Agent

背景信息

云盾数据库审计系统的**系统管理**导航下提供**Agent管理**功能页面，您可以在**Agent管理**页面下载Agent并查看Agent的连接状态。Agent的部署操作在Windows服务器上执行。

操作步骤

1. 登录数据库审计系统。具体操作请参见登录数据库审计系统。
2. 前往**系统管理 > Agent管理**页面。
3. 单击**安装Agent**页签，并在**下载Agent手动安装**区域，单击**Windows**。

4. 在**下载**对话框中，等待打包成功，单击**下载**，下载Windows版Agent安装包。
5. 登录Windows服务器。
6. 将Agent安装包上传到Windows服务器。
7. 将压缩包解压到指定的运行目录。

   说明
   - 解压目录中不能出现空格等特殊字符，具体包括：*<space>*、*()*、*[]*、*{}*、*^*、*=*、*;*、*!*、*'*、*+*、*,*、*`*、*~*、*&*。若一定要在含特殊字符的目录中运行脚本，请选择以管理员权限进入dos命令行运行脚本。
   - 每次更换运行或解压目录时，需要重新运行安装脚本。

8. 进入**dbagent > tool**目录，双击运行*install_npcap.bat*，打开Npcap工具安装向导。Npcap是流量代理运行所依赖的工具，需要优先安装。
9. 根据Npcap工具安装向导，使用默认配置完成Npcap安装。

   说明 您需要管理员权限才能完成Npcap安装。

10. Npcap安装完成后，回到*dbagent*目录，以管理员身份运行*install.bat*，安装并启用Agent程序。

    说明
    - 禁止直接运行二进制文件。
    - 必须以管理员权限运行脚本。
    - 如需自行更改配置文件，请勿更改文件的编码格式。

11. 等待Agent安装完成。Agent安装完成后自动启用。

    说明 安装过程中遇到问题时，建议您尝试以下方法：等待一段时间重试、卸载Agent并重装、重新启动电脑、直接联系我们。

12. Agent程序安装启用后，回到云盾数据库审计系统，前往**系统管理 > Agent管理**页面，在**查看Agent状态**页签下查看Agent的连接状态信息。

    连接状态显示**无异常**，表示成功部署Agent。

    说明 若要强制结束dbagent进程，请先结束monitor进程，再结束agent进程。

更多操作

在Windows环境下，您可以根据需要对已部署的Agent程序执行以下操作：

- 卸载：运行安装目录下的*uninstall.bat*
- 启用：运行安装目录下的*dbagent_start.bat*
- 停用：运行安装目录下的*dbagent_stop.bat*

下一步

部署Agent程序后，您可以前往数据库审计系统的**总览**页面，查看目标数据库的整体安全状态。

8.审计经典网络数据库实例

如果需要审计经典网络数据库实例，您需要先通过ClassicLink功能实现经典网络的ECS与VPC中的数据库审计系统互通，并在经典网络的ECS上部署Agent程序。

经典网络 数据库审计 ClassicLink

前提条件

VPC中启用ClassicLink时，需要满足限定条件，具体请参见ClassicLink概述的使用限制。

背景信息

一般情况下，建议ECS和数据库审计系统处于同一VPC中，具体操作请参见部署Agent程序。

如果您的使用场景比较特殊，ECS需要处于经典网络中，则可以通过ClassicLink功能实现与VPC中的数据库审计系统互通，具体操作请参见本章节。

操作步骤

1. 获取数据库审计系统所在VPC的实例ID。
   i. 登录数据库审计系统。 具体操作请参见登录数据库审计系统。
   ii. 选择**系统管理 > Agent管理**。
   iii. 单击**安装Agent**页签，查看该数据库审计系统所在的VPC实例ID。

2. 创建经典网络中的ECS实例到数据库审计系统所在VPC的ClassicLink连接。
   i. 在数据库审计系统所在VPC中，开启ClassicLink功能，具体请参见开启ClassicLink功能。

   > **说明** 此处操作的VPC实例，请参见步骤步骤1中查看结果。

   ii. 在经典网络的ECS中，建立ClassicLink连接，具体请参见建立ClassicLink连接。 在建立ClassicLink连接操作过程中，选择的VPC实例请参见步骤1中查看的结果。
   iii. （可选）当VPC网段为192.168.0.0/16时，在经典网络ECS中增加192.168.0.0/16指向私网网卡的路由。 具体操作请参见使用限制。

   > **说明** VPC网段为192.168.0.0/16时，需要执行此步骤；VPC网段为其他网段时，不需要执行此步骤。

3. 在经典网络的ECS上手动安装数据库审计系统的Agent程序。
   - 如果ECS为Linux系统，具体请参见Linux系统部署Agent中**下载Agent手动安装**操作。
   - 如果ECS为Windows系统，具体请参见Windows系统部署Agent。
4. 验证是否成功部署Agent程序。
   i. 登录数据库审计系统。 具体操作请参见登录数据库审计系统。
   ii. 选择**系统管理 > Agent管理**。

iii. 单击**查看Agent状态**页签，查看ECS的内网IP是否出现在列表中。

您如果能够在**Agent IP**列表中查看到ECS的内网IP，那么表示连接成功。

9.查询分析

9.1. 审计日志

通过审计日志，您可以查询所有审计数据。本文介绍了在云盾数据库审计系统中查询审计日志的具体操作。

操作步骤

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**查询分析 > 审计日志**。
3. 在**审计日志**页面，设置要查询的**时间范围**和查询条件。

   审计查询功能可以帮助您准确定位到具体操作或语句，您可以参考以下步骤来设置查询条件。

   i. 设置**时间范围**。可选择：**最近5分钟**、**最近30分钟**、**最近1小时**、**最近6小时**、**本日**、**昨天**、**本周**、**本月**和自定义。

   ii. 设置**报文内容**。

   - 如果您要查询的关键字为报文中的参数，那么您可以在**参数关键字**中输入关键字。
   - 如果您要查询的关键字是表名、字段名或者SQL语法中的关键词，可以单击模板后的输入框进行筛选，可筛选项包括**关键词**、**SQL模板ID**、**操作类型**。

   iii. 设置**会话连接**。可根据会话连接信息进行查询，可筛选项包括：**客户端IP**、**客户端端口**、**数据库账号**、**服务端IP**、**服务端端口**、**会话ID**、**客户端工具**、**主机名**、**数据库类型**、**标识状态**。

   iv. 单击**更多条件**可以显示更多筛选条件。可增加的筛选项包括**审计ID**、**数据库名/实例名**、**影响行数**、**执行时长**、**关联IP**、**关联账号**和**执行状态**。

   支持的筛选条件见下表。

筛选项	筛选子项	是否默认显示	说明
报文内容-参数关键字	参数关键字	是	关键字是报文中的参数，支持设置多个关键字，多个关键字之间以空格隔开。
报文内容-模板	关键词	否	关键字为表名、字段名或者SQL语法中的关键词。
	SQL模板ID	否	要查询的SQL模板的ID。
	操作类型	否	SQL的操作类型。 包含Select、Insert、Update等操作类型。
	客户端IP	否	需要连接数据库的客户端的IP地址，支持设置IPv4或IPv6地址。
	客户端端口	否	需要连接数据库的客户端的端口号。

筛选项	筛选子项	是否默认显示	说明
会话连接	数据库账号	否	登录到数据库的账号名称。
	服务端IP	否	数据库服务器服务端的IP地址，支持设置IPv4或IPv6地址。
	服务端端口	否	数据库服务器服务端的端口号。
	会话ID	否	要查询的会话ID。
	客户端工具	否	登录数据库的客户端工具。
	主机名	否	数据库服务器的主机名。
	数据库名/实例名	否	数据库名称或实例名称。
	数据库类型	否	数据库的类型。
	标识状态	否	SQL的执行结果，取值如下： ■ 未知 ■ 登入成功 ■ 登入失败
影响行数	影响行数	是	SQL的影响行数。
执行时长	执行时长	是	SQL的执行时长。
执行状态	执行状态	是	SQL的执行结果，取值如下： ■ 全部（默认取值） ■ 未知 ■ 执行成功 ■ 执行失败
审计ID	审计ID	否	要查询的审计ID。输入多个值时请使用逗号（,）隔开。
数据库名/实例名	数据库名/实例名	否	数据库名称或实例名称。

说明 不同设置条件之间为与的关系。

4. （可选）设置查询条件后，单击**保存**，可以保存查询条件。

保存查询条件后，如果您后续需要使用相同查询条件，不需要重新设置，可以直接在查询条件下拉列表中选择。

5. 单击**搜索**，执行查询。

   > **说明** 一次查询最多可查询10,000条记录。

   完成查询后，在**审计日志**页面下方查看返回记录。

   

6. （可选）您可以单击**设置显示列**图标，并在**设置显示列**对话框中选中要在返回结果中显示的列选项。

   

   

9.2. 告警日志

本文介绍了在云盾数据库审计系统中查询告警日志的具体操作。通过告警日志，您可以查询数据库的告警信息。

操作步骤

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**查询分析 > 告警日志**。
3. 在**告警日志**页面，设置要查询的**时间范围**和查询条件。
   - 时间范围取值：最近5分钟、最近30分钟、最近1小时、最近6小时、本日、本周、本月、自定义。
   - 查询条件支持基础查询和高级搜索。
     - 基础查询：通过设置筛选条件查询相关记录。单击**更多条件**可以显示更多筛选条件。

       支持的筛选条件见下表。

筛选项	是否默认显示	说明
报文	是	在报文中查询关键词。支持设置多个关键词，多个关键词之间以空格隔开。设置多个关键词表示要同时命中多个关键词。
数据库	是	要查询的数据库。
数据库账号	是	登录到数据库的账号名称。
规则名称	是	命中的规则名称。
告警等级	是	触发的告警等级。
审计ID	否	要查询的审计ID。
会话ID	否	要查询的会话ID。
SQL模板ID	否	要查询的SQL模板ID。
数据库类型	否	数据库的类型。

筛选项	是否默认显示	说明
客户端IP	否	客户端的IP地址，支持查询IPv4或IPv6地址。
客户端端口	否	客户端的端口号。
服务端IP	否	服务端的IP地址，支持查询IPv4或IPv6地址。
服务端端口	否	服务端的端口号。
客户端MAC	否	客户端机器的MAC地址。
服务端MAC	否	服务端机器的MAC地址。
数据库名/实例名	否	数据库名称或实例名称。
客户端工具	否	登录数据库的客户端工具。
主机名	否	数据库服务器的主机名。
操作系统用户名	否	客户端操作系统的用户名。
原始SQL长度	否	原始SQL的长度。
影响行数	否	SQL的影响行数。
执行时长	否	SQL的执行时长。
执行结果描述	否	SQL的执行结果描述，仅支持精确查询。
返回结果集	否	SQL的返回结果集，支持模糊查询。
执行状态	否	SQL的执行结果，取值： ■ 全部（默认） ■ 执行成功 ■ 执行失败
操作类型	否	SQL的操作类型。

- 高级搜索：单击**高级搜索**，通过编写**条件表达式**，设置自定义查询条件。在高级搜索页面，单击**条件表达式编写规则**，可以展开或隐藏条件表达式编写规则。

> **说明** 设置查询条件后，单击**保存**，可以保存查询条件。
>
> 已保存的查询条件可以在查询条件下拉框中直接调用。

4. 单击**搜索**，执行查询。

> **说明** 一次查询最多可查询10,000条记录。

5. 在**告警日志**页面下方查看返回记录。

> **说明** 您可以单击**设置显示列**图标，并在**设置显示列**对话框中勾选要在返回结果中显示的列选项。

后续步骤

为数据库配置审计规则

9.3. 会话日志

本文介绍了在云盾数据库审计系统中查询会话日志的具体操作。通过会话日志，您可以查询客户端与服务器端之间建立的会话信息。

操作步骤

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**查询分析 > 会话日志**。
3. 在**会话日志**页面，设置要查询的**时间范围**和查询条件。
   - 时间范围取值：最近5分钟、最近30分钟、最近1小时、最近6小时、本日、本周、本月、自定义。
   - 查询条件支持基础查询和高级搜索。

- 基础查询：通过设置筛选条件查询相关记录。单击**更多条件**可以显示更多筛选条件。

  支持的筛选条件见下表。

筛选项	是否默认显示	说明
数据库	是	要查询的数据库。
数据库账号	是	登录到数据库的账号名称。
客户端IP	是	客户端的IP地址，支持查询IPv4或IPv6地址。
客户端端口	是	客户端的端口号。
服务端IP	是	服务端的IP地址，支持查询IPv4或IPv6地址。
服务端端口	是	服务端的端口号。
会话ID	否	要查询的会话ID。
数据库类型	否	数据库的类型。
客户端MAC	否	客户端机器的MAC地址。
服务端MAC	否	服务端机器的MAC地址。
客户端工具	否	登录数据库的客户端工具。
主机名	否	数据库服务器的主机名。
操作系统用户名	否	客户端操作系统的用户名。
数据库名/实例名	否	数据库名称或实例名称。
状态标识	否	会话状态，取值： ■ 全部 ■ 未知 ■ 登入成功 ■ 登入失败
SQL总记录数	否	SQL的总记录数量。
会话请求总流量	否	会话请求的总流量。
会话返回总流量	否	会话返回的总流量。

- 高级搜索：单击**高级搜索**，通过编写**条件表达式**，设置自定义查询条件。 在高级搜索页面，单击**条件表达式编写规则**，可以展开或隐藏条件表达式编写规则。

> **说明** 设置查询条件后，单击**保存**，可以保存查询条件。
>
> 已保存的查询条件可以在查询条件下拉框中直接调用。

4. 单击**搜索**，执行查询。

> **说明** 一次查询最多可查询10,000条记录。

5. 在**会话日志**页面下方查看返回记录。

> **说明** 您可以单击**设置显示列**图标，并在**设置显示列**对话框中勾选要在返回结果中显示的列选项。

后续步骤

为数据库配置审计规则

10.规则配置

10.1. 为数据库配置审计规则

本文介绍了在云盾数据库审计系统中为数据库配置审计规则的具体操作。

前提条件

已添加数据库。添加数据库的具体操作请参见添加数据库。

背景信息

将数据库添加到数据库审计系统后，您可以为数据库启用审计规则。当审计记录命中启用的审计规则时，会触发告警。

审计规规包括系统规则和用户规则。

- 系统规则为内置规则，包括以下类型：SQL注入规则、漏洞攻击规则、账号安全规则、数据泄露规则、违规操作规则；每种类型下包括多条规则。不同的数据库支持的系统规则不同，具体以数据库的规则配置页面所罗列的可使用规则为准。
- 用户规则为自定义规则，具体内容请参见管理用户规则和白名单。

操作步骤

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**规则配置**。

   规则配置页面显示了已添加到数据库审计系统中的数据库的规则配置概况。每种规则类型下的规则记录（格式为xx/xx）表示：已启用的该类型规则数/可使用的该类型规则数。
3. 定位到要操作的数据库，单击其操作列下的**管理**。

   > **说明** 您也可以单击目标数据库下的任意一个规则记录，进入数据库的规则管理页面。
4. 在目标数据库的**规则管理**页面，通过左侧的规则导航栏，定位到要操作的规则组（系统规则）或规则（用户规则），并单击其名称。
5. 查看规则描述，并根据需要启用/禁用规则。
   - 如果是系统规则，则右侧**规则组**页面显示了该规则组内所有规则的信息；您可以操作**规则列表**中的**启/禁用**开关，启用或禁用具体规则。
   - 如果是用户规则，则右侧**规则**页面显示了该规则的详细信息；您可以操作**状态**后的开关，启用或禁用该规则。
6. （可选）如果启用了多个规则，您可以设置规则优先级。操作步骤如下：
   i. 打开**优先级设置**页签。
   ii. 在**启用的规则列表**中，通过拖动调整规则顺序。顺序越靠前的规则的优先级越高。

   > **说明** 单击重置，可以恢复默认规则排序。

   iii. 单击**保存**。

执行结果

完成规则配置。当目标数据库的审计记录命中启用的审计规则时，会触发告警。您可以前往**查询分析 > 告警日志**页面，查询数据库的告警信息。具体操作请参见告警日志。

后续步骤

管理用户规则和白名单

10.2. 管理用户规则和白名单

本文介绍了在云盾数据库审计系统中管理数据库下的用户规则以及用户规则下的白名单设置的具体操作。

背景信息

用户规则指自定义审计规则。添加数据库后，您可以为其添加用户规则。用户规则在数据库之间互不通用。

添加用户规则后，您可以在为数据库配置审计规则时启用用户规则。这样，当审计记录命中启用的用户规则时，会触发告警。

添加用户规则后，您可以为用户规则添加白名单设置。满足白名单设置的审计记录，即使命中了用户规则，也不会触发告警。

添加用户规则

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**规则配置**。
3. 定位到要操作的数据库，单击其**操作**列下的**管理**。

   > **说明** 您也可以单击目标数据库下的任意一个规则记录，进入数据库的**规则管理**页面。

4. （可选）在目标数据库的**规则管理**页面，根据需要在**用户规则**目录下添加子级目录。

   您可以直接在**用户规则**目录下添加用户规则，或者在用户规则下添加子级目录，然后在子级目录中添加规则。参照以下步骤，添加一个子级目录：

   i. 单击**新增 > 目录**。

   ii. 在**新增目录**侧边页，输入目录**名称**，并在**上级目录**中选择**用户规则**。

   > **说明** 同一个数据库下的所有子级目录的名称不允许重复。

   iii. 单击**保存**。

   成功添加子级目录。您可以在左侧规则导航树中看到已添加的目录。单击一个子级目录进入其信息页；在目录信息页，您可以单击右上角的编辑或删除图标，执行相应操作。

5. 在目标数据库的**规则管理**页面，单击**新增 > 规则**。
6. 在**新增规则**侧边页，完成规则配置（即规则的命中条件），并单击**保存**。规则配置描述见下表。

类别	配置项	支持的逻辑符	说明
基本信息	名称	-	规则名称。 说明 同一数据库下的所有用户规则的名称不允许重复。
	描述	-	规则描述信息。
	等级	-	命中规则后触发的告警等级，取值：高风险、中风险、低风险。
	上级目录	-	规则隶属的上级目录。 说明 只允许在用户规则目录中选择。关于创建用户目录，请参见步骤4。
客户端	客户端IP	等于、不等于	客户端的IP地址。支持填写多个值，多个值之间以逗号（,）分隔。
	客户端工具	等于、不等于	客户端使用的工具名称。支持填写多个值，多个值之间以逗号（,）分隔。例如，db2bp.exe,javaw.exe,plsqldev.exe。
	客户端端口	-	客户端的访问端口号。支持填写多个值或区间，多个值之间以逗号（,）分隔。例如，10-15,20,25,30-40。
	客户端MAC地址	等于、不等于	客户端机器的MAC地址。支持填写多个值，多个值之间以逗号（,）分隔。
	操作系统用户	等于、不等于	客户端操作系统的登录用户名。支持填写多个值，多个值之间以逗号（,）分隔。
	主机名	等于、不等于	客户端的主机名。支持填写多个值，多个值之间以逗号（,）分隔。
服务端	服务端IP	等于、不等于	服务端的IP地址。支持填写多个值，多个值之间以逗号（,）分隔。
	服务端端口	-	服务端的端口号。支持填写多个值或区间，多个值之间以逗号（,）分隔。例如，10-15,20,25,30-40。
	数据库账号	等于、不等于	数据库的登录用户名。支持填写多个值，多个值之间以逗号（,）分隔。例如，system,sys。
	服务端MAC地址	等于、不等于	服务端机器的MAC地址。支持填写多个值，多个值之间以逗号（,）分隔。

类别	配置项	支持的逻辑符	说明
	数据库名（SID）	-	Oracle数据库输入SID，其他数据库输入数据库名称。支持填写多个值，多个值之间以逗号（,）分隔。
行为	操作类型	-	对数据库的操作类型，取值： ○ DDL：Truncate、Create、Alter、Drop、Comment、Rename ○ DML：Select、Insert、Update、Delete、Call、Explain、Lock、Merge ○ DCL：Grant、Revoke
	SQL模板	-	SQL模板的ID。支持填写多个值，多个值之间以逗号（,）分隔。
	SQL关键字	-	配置方式如下： i. 添加条件。 在条件框中输入要匹配的报文内容，支持使用正则表达式。单击**添加条件**可以添加多个条件。 添加一个条件后，您可以执行正则校验，验证指定的内容是否与设置的正则表达式相匹配。操作步骤如下： a. 单击条件下的**正则校验**。 b. 在**正则校验**对话框中，确认**正则表达式**，并输入**校验的内容**。 c. 单击**校验**。 ii. 编写**条件运算逻辑表达式**。 通过与（&）、或（|）、非（~）和括号描述条件间的组合运算关系，条件使用序号表示，例如，“1”表示条件1。 示例： 1&2，表示有两个SQL关键字条件，且两个关键字都要满足，才命中规则并触发告警。
	SQL长度	-	SQL的长度。允许的范围为1字节到64K。
	WHERE子句	-	是否包含WHERE子句，取值：不判断、有WHERE子句、没有WHERE子句。
	执行时长	大于等于、小于等于、区间	SQL的执行时长，单位为微秒。取值范围为0~2147483647。SQL的执行时长属于此范围，则命中规则。
	影响行数	大于等于、小于等于、区间	SQL的影响行数。取值范围为0~2147483647。SQL操作返回的记录数或受影响的行数属于此范围，则命中规则。

类别	配置项	支持的逻辑符	说明
结果	返回结果集	-	配置方式如下： i. 添加条件。 在条件框中输入要匹配的报文内容，支持使用正则表达式。单击**添加条件**可以添加多个条件。 添加一个条件后，您可以执行正则校验，验证指定的内容是否与设置的正则表达式相匹配。操作步骤如下： a. 单击条件下的**正则校验**。 b. 在**正则校验**对话框中，确认**正则表达式**，并输入**校验的内容**。 c. 单击**校验**。 ii. 编写**条件运算逻辑表达式**。 通过与（&）、或（|）、非（~）和括号描述条件间的组合运算关系，条件使用序号表示，例如，“1”表示条件1。 示例： 1&2，表示有两个SQL关键字条件，且两个关键字都要满足，才命中规则并触发告警。
	执行状态	-	执行结果中包含的执行状态，取值：全部、成功、失败。
	执行结果描述	匹配、不匹配	执行结果中包含的关键词，支持以正则表达式的方式进行匹配。
其他	生效时间	-	规则的生效周期，取值：任意时间、每天、每周、每月。

成功添加用户规则。您可以在左侧的规则导航树中看到已添加的用户规则。单击一个用户规则进入其信息页；在用户规则信息页，您可以单击右上角的编辑、删除、克隆图标，执行相应操作。

管理用户规则白名单

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**规则配置**。
3. 定位到要操作的数据库，单击其操作列下的**管理**。
4. 在目标数据库的**规则管理**页面，通过左侧的规则导航树，定位到要操作的用户规则，并单击其名称。
5. 在右侧的规则信息页，单击**白名单**下的**管理**。
6. 在**白名单管理**侧边页，您可以新增白名单。操作步骤如下：
   i. 单击**新增**。

ii. 在**新增白名单**侧边页，完成白名单配置。配置描述如下：

- **名称**：白名单的名称。
- **描述**：白名单的描述。
- 白名单规则：具体的**客户端**、**服务端**、**行为**、**结果**、**其他**配置描述，请参见添加用户规则步骤6中的用户规则配置描述。

iii. 单击**保存**。

成功添加白名单。您可以在**白名单管理**侧边页查看所有白名单。单击一个白名单的操作列下的**编辑**或**删除**，可以执行相应操作。同一个数据库下的所有白名单相互通用，您需要为用户规则引用白名单，才能使白名单设置生效。

7. 在目标规则的规则信息页，单击**白名单**下的**添加**，并从白名单下拉框中选择要引用的白名单。

成功为用户规则引用白名单设置。启用用户规则后，命中白名单设置的审计记录，不会触发告警。

11.报表中心

本文介绍了在云盾数据库审计系统中，如何通过报表中心查看和订阅报表、导出离线报表和管理订阅任务的具体操作。

背景信息

数据库审计系统内置以下三种类型的报表模板，分别从不同角度展示数据库审计的分析结果。

- **塞班斯报表**

  输出 *塞班斯（SOX）法案数据库安全审计符合性报告* ，从计划与组织、确保和控制、评估风险等方面，分析展示数据库的全面安全状况。

- **综合分析报告**

  从SQL语句执行情况、会话连接、风险事件、SQL性能等角度，分析展示数据库的综合状况。

- **性能分析报表**

  从性能变化趋势、性能最差的数据库/SID、耗时最久的SQL、性能最差的SQL、执行最多的SQL等方面，分析展示数据库的性能状况。

查看和订阅报表

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**报表中心**。
3. 在**报表中心**页面，单击要查看的报表页签（**塞班斯报表**、**综合分析报告**或**性能分析报表**）。

   

4. 在报表内容上方，设置查询选项，查看报表内容。 支持设置的查询选项包括以下内容：
   - **数据库**：要查询的数据库。
   - **时间范围**：本日、本周、本月、最近3个月、最近6个月、最近12个月、昨天、上周、上个月、自定义。

     > **说明** 报表的统计粒度与设置的时间范围有关。
     > - 时间范围小于24小时时，报表以小时为单位进行统计。
     > - 时间范围大于24小时且不足40天时，报表以天为单位进行统计。
     > - 时间范围大于40天时，报表以月为单位进行统计。

5. 您可以订阅感兴趣的报表内容，让数据库审计系统以邮件的形式定期向您发送报表。 参照以下步骤，添加一个订阅任务：
   i. 单击报表内容右上角的添加订阅任务图标。

   

ii. 在**添加订阅任务**侧边页，完成订阅任务配置。 订阅任务的配置描述参见下表。

配置项	说明
任务名称	订阅任务的名称。
收件人邮箱	收件人的邮箱地址。支持填写多个地址，多个地址间以逗号（,）分隔。
报表类型	要订阅的报表的类型，取值： ■ 塞班斯报表 ■ 综合分析报告 ■ 性能分析报表
报表格式	要订阅的报表的格式，取值： ■ HTML ■ PDF ■ PNG
数据库	要订阅哪个数据库的报表。
任务周期	订阅任务的邮件发送周期，取值： ■ 每天（日报） ■ 每周（周报） ■ 每月（月报） ■ 每年（年报）
发送时间	根据设置的任务周期，设置邮件发送的具体时间。

iii. 单击**保存**，成功添加订阅任务。

导出离线报表

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**报表中心**。
3. 在**报表中心**页面，单击要查看的报表页签（**塞班斯报表**、**综合分析报告**或**性能分析报表**）。
4. 在报表内容上方，设置查询选项，查看报表内容。 支持设置的查询选项包括以下内容：
   - **数据库**：要查询的数据库。
   - **时间范围**：本日、本周、本月、最近3个月、最近6个月、最近12个月、昨天、上周、上个月、自定义。

> **说明** 报表的统计粒度与设置的时间范围有关。
> - 时间范围小于24小时时，报表以小时为单位进行统计。
> - 时间范围大于24小时且不足40天时，报表以天为单位进行统计。
> - 时间范围大于40天时，报表以月为单位进行统计。

5. 您可以将需要离线使用的报表内容导出成HTML、PDF、PNG文件。 参照以下步骤，导出报表内容：
   i. 单击报表内容右上角的导出报表图标。

   

   ii. 在导出报表菜单中，选择导出报表的格式：HTML（推荐使用）、PDF、PNG。

   

   iii. 等待导出文件生成，在**下载**对话框中，单击**下载**。

   

   成功下载报表文件。

管理订阅任务

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**报表中心**。
3. 在**报表中心**页面，单击**管理订阅任务**。
4. 在**管理订阅任务**页面，根据需要添加、编辑、删除订阅任务。

   

   - 添加订阅任务
     a. 单击订阅任务列表上方的**添加**。
     b. 在**添加订阅任务**侧边页，完成订阅任务配置。订阅任务的配置描述请参见配置说明。
     c. 单击**保存**。

     成功添加订阅任务。已添加的订阅任务显示在订阅任务列表中。数据库审计系统会定期将订阅的报表发送到指定邮箱。
   - 编辑订阅任务
     a. 在订阅任务列表中，定位到要编辑的订阅任务，单击其操作列下的**编辑**。
     b. 在**编辑订阅任务**侧边页，修改订阅任务配置。订阅任务的配置描述请参见配置说明。
     c. 单击**保存**。

     成功修改订阅任务。
   - 删除订阅任务
     a. 在订阅任务列表中，定位到要删除的订阅任务，单击其操作列下的**删除**。
     b. 在确定删除订阅任务对话框中，单击**确定**。

     成功删除订阅任务。

12.系统管理

本文介绍了在云盾数据库审计系统中设置系统管理的具体操作。您可以在系统管理下管理数据库和Agent，或重置偏好设置。

数据库管理

数据库是云盾数据库审计系统的审计对象。您必须在数据库审计系统中添加数据库，才能为数据库启用审计服务。

操作步骤

登录云盾数据库审计系统（具体操作请参见登录数据库审计系统），并前往**系统管理 > 数据库管理**页面。

您可以在**数据库管理**页面添加要审计的数据库，或查看、编辑、删除已添加的数据库。具体操作请参见管理数据库。

Agent管理

云盾数据库审计系统的Agent程序是安装在数据库服务器上的用于采集数据库流量的工具。您必须在数据库服务器上部署Agent程序，才能使数据库审计服务收集审计数据。

操作步骤

登录云盾数据库审计系统（具体操作请参见登录数据库审计系统），并前往**系统管理 > Agent管理**页面。

您可以在**Agent管理**页面安装Agent或查看Agent状态。具体操作请参见部署Agent程序。

重置配置

通过重置配置，您可以将数据库审计系统中与界面显示相关的配置（例如，表格的显示列等）恢复到默认设置。界面显示的相关配置保存在您的浏览器设置中。

操作步骤

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**系统管理 > 重置配置**。
3. 在**偏好设置**下，单击**重置**。
4. 在确认重置对话框中，单击**确定**。

成功重置偏好设置，所有与界面显示相关的配置恢复到默认设置。